1. Finite Fields

The first examples of finite fields are quotient fields of the ring of integers $\mathbb{Z}$: let $t > 1$ and define $\mathbb{Z}_{/t} = \mathbb{Z}/(t\mathbb{Z})$ to be the ring of congruence classes of integers modulo t: in practical terms, we identify the clases with the remainders $\{0, 1, \cdots, t-1\}$ and define the sum and product modulo t. Then $\mathbb{Z}_t$ is a field iff t is a prime. For a prime q, we denote this field by $\mathbb{F}_q$. Some general properties of these fields are necessarily shared by all finite fields. They are reviewed in the next sections.

1.1. **The Additive structure of Finite Fields.** Let $\mathbb{F}$ be any finite field with sum $a+b$ and multiplication ab, for all $a, b \in \mathbb{F}$. There exist necessarily two distinct elements in $\mathbb{F}$, the 0 (defined as the unique element such that $0 + a = a + 0 = a$ for all $a \in \mathbb{F}$) and the 1 (defined as the unique element such that $1a = a1 = a$ for all $a \in \mathbb{F} \setminus \{0\}$). The multiplicative subgroup of non-zero elements of $\mathbb{F}$ is denoted by $\mathbb{F}^\times$.
There is a naturally defined homomorphism of rings from $\mathbb{Z}$ to $\mathbb{F}$

$$\psi : \mathbb{Z} \to \mathbb{F} : \psi(t) = t \cdot 1 = \begin{cases} \sum_{i=1}^{t} 1 & \text{if } t > 0 \\ -\sum_{i=1}^{-t} 1 & \text{if } t < 0 \\ 0 & \text{if } t = 0 \end{cases}$$

We denote $\psi(t)$ simply as t.
The kernel of ψ is an ideal $q\mathbb{Z} \subset \mathbb{Z}$, with $q > 0$ necessarily a prime, as otherwise, if $q = st$ with both $s > 1$ and $t > 1$, $0 = \psi(st) = \psi(s)\psi(t)$ and $\mathbb{F}$ would contain divisors of zero.

We conclude that there exists a injective homomorphism of $\mathbb{F}_q$ into $\mathbb{F}$ and, identifying $\mathbb{F}_q$ with its image, we may consider $\mathbb{F}_q$ as a subfield of $\mathbb{F}$; it is called the **prime subfield** of $\mathbb{F}$ and q is called the **characteristic** of $\mathbb{F}$.
This implies that $\mathbb{F}$ is a vector space over $\mathbb{F}_q$ of finite dimension m and so $|\mathbb{F}| = q^m$. This field is denoted as $\mathbb{F}_{q^m}$, a notation that hints, implicitely, to the fact that a finite field with that given cardinality is essentially unique. When there is no ambiguity, we will denote this field simply as $\mathbb{F}$, but will use sistematically the notation $\mathbb{F}_q$ for the prime fields.
The vector space structure described above completely determines the additive structure of $\mathbb{F}$: it is isomorphic to a direct product of m copies of $\mathbb{F}_q$; given a basis $u_1, \cdots, u_m$, the elements of $\mathbb{F}$ may be identified with the corresponding vectors of coordinates with respect to that basis and sum is performed component wise.

1.2. **Multiplicative structure: Orders and Primitive Elements.** Let again $\mathbb{F} = \mathbb{F}_{q^m}$. The understanding of the multiplicative structure of $\mathbb{F}$ starts with the following basic property:

Proposition 1 (Fermat/Euler)**.** *For every $a \in \mathbb{F}^\times$, $a^{q^m-1} = 1$. Equivalentely, for every $a \in \mathbb{F}$, $a^{q^m} = a$.*

Proof. The equivalence of both statements is obvious. Suppose $a \neq 0$ and let the nonzero elements of the field be indexed as a_i, $1 \leq i < q^m$. The mapping

$$\mathbb{F}^\times \to \mathbb{F}^\times, \qquad a_i \to a a_i$$

is a bijection. So

$$a^{q^m-1}\prod_{i=1}^{q^m-1} a_i = \prod_{i=1}^{q^m-1} aa_i = \prod_{i=1}^{q^m-1} a_i,$$

which implies the result, because $\prod_{i=1}^{q^m-1} a_i \neq 0$. □

Definition 2. *For any $a \in \mathbb{F}^\times$, the order of a is defined as*

$$\mathrm{ord}(a) = \min\{k > 0 : a^k = 1\}.$$

Proposition 3. *For any $a, b \in \mathbb{F}^\times$,*

i) $\mathrm{ord}(a) \mid (q^m - 1)$*;*
ii) $\mathrm{ord}(a^j) = \frac{\mathrm{ord}(a)}{\gcd(j,\mathrm{ord}(a))}$*;*
iii) *If* $\mathrm{ord}(a) = s$, $\mathrm{ord}(b) = t$ *and* $\gcd(s,t) = 1$, *then* $\mathrm{ord}(ab) = st$.

Proof. **HW**. □

Remark 4. *The definition and properties of multiplicative order are generalized for elements of a general commutative finite group. In particular, given a positive integer m, we define, for any a prime to m,*

$$\mathrm{ord}_m(a) = \min\{k > 0 : a^k \equiv 1 \mod m\} = \min\{k > 0 : m \mid (a^k - 1)\}.$$

We now consider the problem of computing the number of elements in a finite field, with a given order. For each $t \mid (q^m - 1)$ let $O(t) = \{a \in \mathbb{F}^\times : \mathrm{ord}(a) = t\}$.

Assume $O(t) \neq \emptyset$ and $a \in O(t)$; then $\{a, a^2, \cdots, a^{t-1}\}$ are distinct roots of $x^t - 1$. But a polynomial over a field can not have more roots than its degree (a fact to be verified below); and as any $b \in O(t)$ is also a root of that polynomial, we conclude, taking into account the properties of the order, that, if $O(t)$ is nonempty,

$$O(t) = \{a^j : 1 \leq j < t; \gcd(j,t) = 1\},$$

and $|O(t)| = \phi(t)$, where ϕ denotes the Euler function. Therefore,

$$q^m - 1 = |\mathbb{F}^\times| = \sum_{t|(q^m-1)} |O(t)| \leq \sum_{t|(q^m-1)} \phi(t).$$

We recall that Euler's ϕ function is, by definition, a **multiplicative** function: if $\gcd(m,n) = 1$ then $\phi(mn) = \phi(m)\phi(n)$ (**HW**). From this observation, and from the easily confirmed fact that for a prime q, $\phi(q^k) = q^k - q^{k-1}$, we obtain the general formula

$$\phi(n) = \phi\left(\prod_{i=1}^r q_i^{t_i}\right) = \prod_{i=1}^r \left(q_i^{t_i} - q_i^{t_i-1}\right) = n\prod_{i=1}^r \left(1 - \frac{1}{q_i}\right)$$

Moreover, $\sum_{t|n} \phi(t) = n$ for any n.

Exercise 5. *Prove that $\sum_{t|n} \phi(t) = n$ for any n, by induction on the number of distinct prime divisors of n.*

Back to our problem, we conclude that $|O(t)| = \phi(t)$ for every $t \mid (q^m - 1)$ (ie, $O(t)$ is always non-empty). In particular, we obtain the following result:

Proposition 6. *If $\mathbb{F} = \mathbb{F}_{q^m}$, there exist exactly $\phi(q^m - 1)$ elements $a \in \mathbb{F}^\times$ with order* $\mathrm{ord}(a) = q^m - 1$.

An $\alpha \in \mathbb{F}^\times$ with order $\mathrm{ord}(\alpha) = q^m - 1$ is called a **primitive element** or **primitive root** of the field.
The multiplicative structure of $\mathbb{F}$ is in this way completely determined: $\mathbb{F}^\times$ is a cyclic group (of order $q^m - 1$) $\{\alpha^i : 0 \le i < q^m\}$.
When a primitive element α is known, multiplications in the field are turned into sums by means of a "table of logarithms": for any $c, d \in \mathbb{F}^\times$

$$cd = \alpha^s \alpha^t = \alpha^{s+t}.$$

Example 7. *2 is a primitive element of $\mathbb{F}_{11}$; the following table presents the correspondance between exponents $0 \le j < 10$ in the first row and field elements 2^j in the second:*

0	1	2	3	4	5	6	7	8	9
1	2	4	8	5	10	9	7	3	6

It is easy to see that if α is a primitive element then α^j is primitive if and only if $\gcd(j, q^m - 1) = 1$ (**HW**).

The following map, the **Frobenius automorphism** of $\mathbb{F}$ over $\mathbb{F}_q$, is essential for the theory:

Proposition 8. *Let $\sigma : \mathbb{F} \to \mathbb{F}$ be defined by $\sigma(a) = a^q$. Then σ is a field automorphism, ie, it is bijective and satisfies $\sigma(a + b) = \sigma(a) + \sigma(b)$ and $\sigma(ab) = \sigma(a)\sigma(b)$. Furthermore, $\sigma(a) = a$ iff $a \in \mathbb{F}_q$.*

Proof. **HW**. □

In order to construct non-prime finite fields and to understand their properties, we need to consider in some detail polynomials in one variable.

1.3. **Polynomials over $\mathbb{F}$.** In this subsection $\mathbb{F}$ denotes a field, not necessarily finite. Denote by $\mathbb{F}[x]$ the ring and $\mathbb{F}$-vector space of polynomials (in a variable x) with coefficients in $\mathbb{F}$:

$$\mathbb{F}[x] = \{p(x) = \sum_{k \ge 0} a_k x^k \,|a_k \in \mathbb{F}; \exists M : a_k = 0 \forall k > M\}$$

If $a_m \neq 0$ and $a_k = 0\ \forall k > m$, $m = \deg(p(x))$ is the **degree** of $p(x)$;
if $m = \deg(p(x))$ and $a_m = 1$, $p(x)$ is **monic**. Obviously, for every nonzero polynomial $p(x) \in \mathbb{F}[x]$ there exists unique $a \in \mathbb{F}^\times$ and monic $g(x)$ such that $p(x) = ag(x)$.

The notation $p(x) = \sum_{k \ge 0} a_k x^k$ (with no explicit reference to the degree) simplifies the presentation of the formulas for algebraic operations:
If

$$f(x) = \sum_{k \ge 0} a_k x^k, \qquad g(x) = \sum_{k \ge 0} b_k x^k,$$

then

$$(f + g)(x) = \sum_{k \ge 0} (a_k + b_k) x^k,$$

$$f \cdot g(x) = \sum_{k \ge 0} \left(\sum_{j=0}^{k} a_j b_{k-j} \right) x^k;$$

the multiplication by a scalar $c \in \mathbb{F}$ is a particular case ($c \neq 0$ is a polynomial of degree 0):

$$cf(x) = \sum_{k \geq 0} (ca_k)x^k.$$

The well known division algorithm of polynomials shows that

Lemma 9. *For any $f(x), g(x) \in \mathbb{F}[x]$, with $g(x)$ not the zero polynomial, there exist unique polynomials $u(x)$ and $r(x)$ satisfying*

$$f(x) = u(x)g(x) + r(x), \qquad deg(r(x)) < deg(g(x)).$$

If $r(x) = 0$, we say that $g(x)$ divides $f(x)$: $g(x) \mid f(x)$.
On the basis of this division Lemma, an Euclidean algorithm is defined, giving rise to the proof of the existence of the $\gcd(f(x), g(x))$ of two nonzero polynomials, similarly to what happens in $\mathbb{Z}$. If

i) $h(x) \mid f(x), h(x) \mid g(x)$ and
ii) $(v(x) \mid f(x) \wedge v(x) \mid g(x)) \implies v(x) \mid h(x)$,

then also $ch(x)$ has the same property, for any $c \in \mathbb{F}^\times$. We thus define $\gcd(f(x), g(x))$ as the unique monic polynomial satisfying i) and ii).
Again as in $\mathbb{Z}$, there exist polynomials $u(x)$ and $v(x)$ such that

$$\gcd(f(x), g(x)) = u(x)f(x) + v(x)g(x),$$

that may be determined using the **extended Euclidean algorithm**: denoting $r_{-1}(x) = f(x)$ and $r_0(x) = g(x)$, the algorithm computes, applying the division algorithm, a sequence of remainders

$$r_{k+1}(x) = r_{k-1}(x) - q_{k+1}(x)r_k(x),$$

and a pair of sequences $u_k(x)$ and $v_k(x)$ satisfying

$$r_k(x) = u_k(x)f(x) + v_k(x)g(x);$$

by a simple computation and induction argument, it is easy to verify that these may be obtained by the initial conditions and recurrence relations

$$u_{-1}(x) = 1 \qquad u_0(x) = 0 \qquad u_{k+1}(x) = u_{k-1}(x) - q_{k+1}(x)u_k(x)$$

$$v_{-1}(x) = 0 \qquad v_0(x) = 1 \qquad v_{k+1}(x) = v_{k-1}(x) - q_{k+1}(x)v_k(x).$$

Furthermore,

Lemma 10. *The quotients $q_k(x)$, remainders r_k and coefficients u_k and v_k obtained in the extended Euclidean algorithm applied to $f(x), g(x) in \mathbb{F}[x]$ satisfy, for all k,*

i) $u_k(x)v_{k+1}(x) - u_{k+1}(x)v_k(x) = (-1)^{k+1}$;
ii) $r_k(x)v_{k+1}(x) - r_{k+1}(x)v_k(x) = (-1)^{k+1}f(x)$;
iii) $r_{k+1}(x)u_k(x) - r_k(x)u_{k+1}(x) = (-1)^{k+1}g(x)$;
iv)
- $\deg(u_k(x)) = \sum_{i=2}^{k} \deg(q_i(x))$,
- $\deg(v_k(x)) = \sum_{i=1}^{k} \deg(q_i(x))$,
- $\deg(r_k(x)) = \deg(f(x)) - \sum_{i=1}^{k+1} \deg(q_i(x))$.

Proof. **(HW)**. □

Example 11. *Let* $q = 13$ *and*

$$f(x) = 7x^6 + 5x^4 + x + 2,\ g(x) = 4x^5 + 5x^3 + 3x^2 + 6.$$

The following table presents the simultaneous calculations for the sequence of remainders and of the polynomials $u_k(x)$ *and* $v_k(x)$*:*

r_i	q_i	u_i	v_i
$7x^6 + 5x^4 + x + 2$		1	0
$4x^5 + 5x^3 + 3x^2 + 6$		0	1
$6x^4 + 11x^3 + 10x + 2$	$5x$	1	$8x$
$4x^3 + 5x^2 + 8x + 7$	$5x + 6$	$8x + 7$	$12x^2 + 4x + 1$
$8x^2 + 12x + 4$	$8x + 9$	$x^2 + 2x + 3$	$8x^3 + 3x^2 + 3x + 4$
$x + 1$	$7x + 8$	$6x^3 + 4x^2 + 10x + 9$	$9x^4 + 6x^3 + 6x^2 + 4x + 8$
0	$8x + 4$	$4x^4 + 9x^3 + 9x^2 + 7x + 6$	$6x^5 + 7x^4 + x^3 + 12x^2 + x + 11$

We conclude that $d(x) \equiv x + 1$ *is the greatest common divisor of* $f(x)$ *and* $g(x)$*, in the ring* $\mathbb{Z}_{/13}[x]$*, and we have the equality*

$$x + 1 \equiv (6x^3 + 4x^2 + 10x + 9)f(x) + (9x^4 + 6x^3 + 6x^2 + 4x + 8)g(x).$$

Definition 12. $f(x) \in \mathbb{F}[x]$ *with positive degree is* ***irreducible*** *if* $f(x) = g(x)h(x)$ *implies that at least one of these factors is a constant (a degree* 0 *polynomial).*

Monic irreducible polynomials play the same role in $\mathbb{F}[x]$ that primes do in $\mathbb{Z}$. In particular,

Proposition 13. *If* $f(x)$ *is monic and irreducible, and* $f(x) \mid g(x)h(x)$ *then* $f(x)$ *divides one of the factors in the product.*

Proof. **HW**. □

And we have a version of the Fundamental Theorem of Arithmetic:

Theorem 14. *Each monic polynomial has a unique, up to order of the factors, decomposition as a product of monic irreducible polynomials.*

Proof. **HW**. □

Definition 15. $a \in \mathbb{F}$ *is called a root of* $f(x) \in \mathbb{F}[x]$ *if* $f(a) = 0$ *(considering* $f(x)$ *as a function on* $\mathbb{F}$*) or, equivalentely, if* $(x - a) \mid f(x)$*.*

By induction on the degree, for instance, one proves that

Proposition 16. *If* $deg(f(x)) = k > 0$ *then* $f(x)$ *has no more than* k *roots (counted with multiplicity).*

Proof. **HW**. □

Remark 17. *An obvious corollary is that a degree* k *polynomial over a field has no more than* k *distinct roots. This corollary has an independent and almost immediate proof, which is left as an exercise also.*

Later we will study in detail the factorization of polynomials over finite fields. For the moment, we notice an important special case:

Definition 18. *A polynomial $f(x) \in \mathbb{F}[x]$ is said to **split completely** if it decomposes as a product of distinct linear factors.*

Proposition 19. *If $\mathbb{F}$ is a field with q^m elements, the polynomial $x^{q^m} - x$ splits completely in $\mathbb{F}[x]$*

Proof. **HW**. □

1.4. **Construction of Extensions of $\mathbb{F}_q$.** The existence and explicit construction of finite fields other than the prime fields follows from the following result:

Proposition 20. *Let $f(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree m. Then the quotient ring $\mathbb{F}_q[x]/(f(x))$ is a field with q^m elements.*

Proof. **HW**. □

This field may be seen, in an informal way, as the set of polynomials with coefficients in $\mathbb{F}_q$ and degree less than m (the remainders upon division by $f(x)$), with the operations of sum and product done modulo $f(x)$.
It is more convenient to denote by a new symbol, say β, the congruence class of x in the quotient and identify $\mathbb{F}$ with $\mathbb{F}_q[\beta]$, the field obtained from $\mathbb{F}_q$ by adding the "new" element β; this new element satisfies $f(\beta) = 0$ and this equality determines the operations of sum and product: $1, \beta, \cdots, \beta^{m-1}$ is a basis of $\mathbb{F}$ over $\mathbb{F}_q$; given $a, b \in \mathbb{F}$

$$a = \sum_{i=0}^{m-1} s_i \beta^i, \; b = \sum_{i=0}^{m-1} t_i \beta^i \quad \text{with } a_i, b_i \in \mathbb{F}_q$$

the sum and product are obtained as the usual sum and product of the polynomial expressions; the product, which is a polynomial expression of degree less or equal than $2m-2$ is then reduced to a linear combination of the powers β^i, $0 \leq i < m$, by the repeated use of the equality $f(\beta) = 0$.
It should be noticed, however, that $\mathbb{F} = \mathbb{F}_q[\beta]$ does not imply that β is a primitive element of the field: take, for example, $\mathbb{F}_3[x]/(x^3 + x^2 + 2)$.

Remark 21. *This construction of the field $\mathbb{F}$ as a finite algebraic extension of $\mathbb{F}_q$, is no different from the maybe more familiar extensions of the rational field, as $\mathbb{Q}[\sqrt{2}] \simeq \mathbb{Q}[x]/(x^2-2)$, which may appear "more natural" only because we consider, implicitely, $\mathbb{Q}$ as a subfield of the algebraically closed field $\mathbb{C}$, where $\sqrt{2}$ exists, so to speak. However, as in our case, that extension of the rationals is completely independent of this inclusion and is valid also inside other algebraic completions of $\mathbb{Q}$, such as the p-adic fields.*

Example 22. *The simplest of all non-trivial examples of this construction is the following: $x^2+x+1 \in \mathbb{F}_2[x]$ is irreducible. We may then represent $\mathbb{F} = \mathbb{F}_2[x]/(x^2 + x + 1)$ as $\mathbb{F} = \{0, 1, \beta, \beta + 1\}$. The sum and product tables are easily deduced: for instance $\beta(\beta + 1) = 1$, etc.*

Example 23. *We consider the field $\mathbb{F}_{27} \simeq \mathbb{F}_3[x]/(x^3+2x+2)$ which can be identified with*

$$\mathbb{F}_3[\alpha] = \{a + b\alpha + c\alpha^2 : a, b, c \in \mathbb{F}_3\}$$

where α satisfies $\alpha^3 = \alpha + 1$.

For example,

$$\alpha(\alpha^2 + \alpha + 1) = \alpha^3 + \alpha^2 + \alpha = \alpha + 1 + \alpha^2 + \alpha = \alpha^2 + 2\alpha + 1.$$

To compute $(\alpha + 1)^{-1}$, we solve $(\alpha + 1)(a + b\alpha + c\alpha^2) = 1$.

$$(\alpha + 1)(a + b\alpha + c\alpha^2) = a + (a + b)\alpha + (b + c)\alpha^2 + c\alpha^3 =$$

$$= a + (a + b)\alpha + (b + c)\alpha^2 + c(\alpha + 1) = (a + c) + (a + b + c)\alpha + (b + c)\alpha^2$$

But

$$(a + c) + (a + b + c)\alpha + (b + c)\alpha^2 = 1 \Leftrightarrow \begin{cases} a + c = 1 \\ a + b + c = 0 \\ b + c = 0 \end{cases}$$

So $(\alpha + 1)^{-1} = 2\alpha + \alpha^2$.

The same reasoning may be applied starting with any finite field $\mathbb{F}$: if $f(x) \in \mathbb{F}[x]$ is irreducible with degree d, $\mathbb{F}' = \mathbb{F}[x]/(f(x))$ is a degree d extension of $\mathbb{F}$. Of course, if $\mathbb{F}$ is a degree m extension of a prime field $\mathbb{F}_q$, $\mathbb{F}'$ is a degree dm extension of $\mathbb{F}_q$. We will confirm that, for each q and m there exists, up to isomorphism, only one extension of $\mathbb{F}_q$ with degree m.
On the other hand, given a fixed extension $\mathbb{F}_{q^m}$, we have

Proposition 24. *$\mathbb{F}_{q^m}$ contains a unique subfield $\mathbb{F}_{q^d}$ for each $d \mid m$ and these are the only subfields of $\mathbb{F}_{q^m}$.*

Proof. The theorem of Fermat-Euler shows that $x^{q^d} - x$, because it divides $x^{q^m} - x$, splits completely in $\mathbb{F}_{q^m}$ as a product of linear factors. Applying the Frobenius automorphism of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ confirms that the roots of that polynomial are a subfield.
The last statement is an immediate consequence of the properties of the order.
□

The construction of finite extensions of $\mathbb{F}_q$ depends on the existence and knowledge of irreducible polynomials $f(x) \in \mathbb{F}_q[x]$.

1.4.1. *Counting Irreducible Polynomials.* We start with some general facts about arithmetic functions:

Definition 25. *A function $f : \mathbb{N} \to \mathbb{C}$ is **multiplicative** if $f(mn) = f(m)f(n)$ for any* coprime *integers m and n.*

Proposition 26. *If $f : \mathbb{N} \to \mathbb{C}$ is a multiplicative function, then*

$$F : \mathbb{N} \to \mathbb{C}, \qquad F(n) = \sum_{d|n} f(d)$$

is also multiplicative.

Proof. **HW**. □

Definition 27 (Möbius Function)**.** *The Möbius function* $\mu : \mathbb{N} \to \{-1, 0, 1\}$ *is defined as*

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n \text{ is squarefree with } k \text{ distinct prime factors} \\ 0 & \text{otherwise} \end{cases}$$

The function μ is obviously multiplicative and it satisfies the following

Theorem 28. *For any* $n \in \mathbb{N}$

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$$

Proof. For $n = 1$ the result is obvious. Suppose that $n > 1$ and, if n has the prime factorization $n = \prod_{i=1}^{t} p_i^{k_i}$ (with $k_i > 0$), define $rad(n) = \prod_{i=1}^{t} p_i$. It is clear

$$\sum_{d|n} \mu(d) = \sum_{d|rad(n)} \mu(d)$$

as for other divisors of n the corresponding summand is zero by definition. This sum may be written, taking the number of factor primes of d as a parameter, as

$$\sum_{d|rad(n)} \mu(d) = \sum_{j=0}^{t} \binom{t}{j} (-1)^j = 0$$

by Newton's Binomial formula. □

The main property of the Möbius function is expressed in the following fundamental result:

Theorem 29 (Möbius Inversion Formula)**.** *Given* $f : \mathbb{N} \to \mathbb{N}$*,*

$$F(n) = \sum_{d|n} f(d) \Leftrightarrow f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

Proof. The proof consists in a straightforward computation:

$$\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{t|n/d} f(t) = \sum_{t|n} f(t) \sum_{d|n/t} \mu(d) = f(n)$$

as a consequence of the previous theorem.
The converse is proved in the same way. □

A similar argument proves

Theorem 30. *Given* $f : \mathbb{N} \to \mathbb{N}$*,*

$$F(n) = \prod_{d|n} f(d) \Leftrightarrow f(n) = \prod_{d|n} \left(F\left(\frac{n}{d}\right)\right)^{\mu(d)}.$$

Proof. **HW**. □

The Inversion Formula is used to disclose several formulas for arithmetical functions and relations between them.
Here we apply this theorem to obtain a formula for the number of irrreducible polynomials, of given degree n, over a prime field $\mathbb{F}_q$:
denote this number as $I_q(n)$; we saw before that $x^{q^m} - x$ factors over $\mathbb{F}_q$ as the product of all monic irreducible polynomials with degree dividing m; equating degrees, we have

$$q^m = \sum_{d|m} dI_q(d).$$

Möbius Inversion formula implies

Proposition 31. *Let q be a prime. For any $n \in \mathbb{Z}^+$, the number of irreducible polynomials of degree n in $\_q[x]$ is*

$$I_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}.$$

In particular, $I_q(n) > 0$, thus assuring the existence of irreducible polynomials and so of field extensions of $\mathbb{F}_q$ of any given degree.

1.4.2. *Minimal polynomials.*

Definition 32. *Given $a \in \mathbb{F} = \mathbb{F}_{q^m}$, the **minimal polynomial** of a over $\mathbb{F}_q$ is the (unique) monic polynomial $p_a(x) \in \mathbb{F}_q[x]$ of minimum degree such that $p_a(a) = 0$.*

We state several properties of minimal polynomials:

Proposition 33.
1. *$p_a(x)$ exists and is unique;*
2. *$p_a(x)$ is irreducible;*
3. *If $p(x) \in \mathbb{F}_q[x]$ is a monic irreducible polynomial and $p(a) = 0$ for some $a \in \mathbb{F}$, then $p(x) = p_a(x)$;*
4. *$p_a(x) \mid x^{q^m} - x$ and so $deg(p_a(x)) \mid m$;*
5. *if α is a primitive element of $\mathbb{F}_{q^m}$ then $deg(p_\alpha(x)) = m$.*

Proof. The second part of 4. will be a consequence of a proposition in the next section. The proof of the other statements is left as an exercise. □

The first example of a minimal polynomial was already provided by the construction of $\mathbb{F} = \mathbb{F}_q[\beta] = \mathbb{F}_q[x]/(f(x))$ itself, as it is easily seen that $f(x)$ is the minimal polynomial of β (and of course of the other roots β^{q^s}). More generally, minimal polynomials of elements of $\mathbb{F}_{q^m}$ are exactly the irreducible polynomials with coefficients in $\mathbb{F}_q$ and degree dividing m.

Remark 34. *We notice that, as a consequence of 5. in the previous proposition, the construction of a finite field as the quotient of the polynomial ring $\mathbb{F}_q[x]$ by the ideal generated by a monic irreducible polynomial $f(x)$ of degree m gives rise to all possible finite fields $\mathbb{F}$ of cardinality q^m: suppose $\mathbb{F}$ is a finite extension of $\mathbb{F}_q$ and α a primitive element with minimal polynomial $p(x)$. Then $\mathbb{F} = \mathbb{F}_q[\alpha] \simeq \mathbb{F}_q[x]/(p(x))$.*

1.5. **Factorizations of Polynomials.** We focus our study of finite fields on the problem of factorization of polynomials, which is also essential for the applications to follow. This may be done, with advantage, in the framework of a general finite field $\mathbb{F}_N$ (where, of course, N is a prime power) and its extensions.
It is convenient to generalize the definition of the Frobenius automorphism:

Definition 35. *Given a finite field $\mathbb{F}_N$ and an extension $\mathbb{F}_{N^m}$, the Frobenius automorphism of the extension is the mapping*

$$\sigma : \mathbb{F}_{N^m} \to \mathbb{F}_{N^m}, \qquad \sigma(x) = x^N.$$

It satisfies

$$\sigma(x+y) = \sigma(x) + \sigma(y), \qquad \sigma(xy) = \sigma(x)\sigma(y),$$

and

$$\sigma(x) = x \Leftrightarrow x \in \mathbb{F}_N$$

Exercise 36. *Verify that σ has the stated properties. Hint: remember that $N = q^t$ for some prime q.*

Remark 37. *Only if we need to identify the extension for which the automorphism is defined, we use the more detailed notation $\sigma_{[\mathbb{F}_{N^m}:\mathbb{F}_N]}$.*

Remark 38. *The Frobenius automorphism of the extension of $\mathbb{F}_N$ by $\mathbb{F}_{N^m}$ induces an automorphism of the ring $\mathbb{F}_{N^m}[x]$, which we denote again by σ, by the formula*

$$\sigma\left(\sum_i a_i x^i\right) = \sum_i \sigma(a_i) x^i.$$

Exercise 39. *Verify that the mapping defined in the previous remark is a ring automorphism*

$$\sigma(g(x)+h(x)) = \sigma(g(x)) + \sigma(h(x)), \qquad \sigma(g(x)h(x)) = \sigma(g(x))\sigma(h(x)),$$

and that $\sigma(g(x)) = g(x)$ if and only if $g(x) \in \mathbb{F}_N[x]$.

1.5.1. *Order and degree of irreducible polynomials.* Given an irreducible polynomial $f(x)$, and the corresponding field $\mathbb{F}_q[\beta]$, as above, we have

Claim 40. *$f(x)$ **splits completely** over $\mathbb{F}_q[\beta]$, ie, it decomposes as the product of* distinct *degree* 1 *factors*

$$f(x) = \prod_{s=0}^{m-1} (x - \beta^{q^s}).$$

Proof. **HW**. **Hint:** Use the Frobenius automorphism. □

Proposition 41. *The roots of $f(x)$ have all the same order.*

Proof. Let $\mathrm{ord}(\beta) = d$; we have $\mathrm{ord}(\beta^{q^s}) = \frac{d}{\gcd(q^s,d)}$. But $d \mid (q^m - 1)$ and obviously $q^m - 1$ and q^s are coprime.

□

As we will see now, $f(x) \mid (x^{q^m} - x)$:

Proposition 42. *If $h(x) \in \mathbb{F}_q[x]$ is irreducible and $deg(h(x)) = t$ then*

$$h(x) \mid (x^{q^m} - x) \text{ iff } t \mid m.$$

Proof. Let $\mathbb{F} = \mathbb{F}_q[x]/(h(x)) = \mathbb{F}_q[\beta]$ and consider the equality

$$x^{q^m} - x = u(x)h(x) + r(x),$$

with $deg(r(x)) < t$. Suppose first that $t \mid m$. We have that, for any $c \in \mathbb{F}$ and every $j > 0$, $c^{q^{tj}} = c$ (**HW**); in particular, $c^{q^m} = c$ for all $c \in \mathbb{F}$. This implies that the t distinct roots of $h(x)$ in $\mathbb{F}$ must also be roots of $r(x)$, which can happen only if $r(x) = 0$.
Conversely, suppose that $h(x) \mid (x^{q^m} - x)$; this implies that $\sigma^m(\beta) = \beta^{q^m} = \beta$. Let α be a primitive element of $\mathbb{F}$ (ie, an element of $\mathbb{F}$ with order $q^t - 1$); there exist $v_l \in \mathbb{F}_q$, $0 \leq l < t$, such that $\alpha = \sum_{l=0}^{t-1} v_l \beta^l$; applying the Frobenius automorphism again

$$\sigma^m(\alpha) = \sum_{l=0}^{t-1} v_l \sigma^m(\beta^l) = \sum_{l=0}^{t-1} v_l \beta^l = \alpha.$$

So $\alpha^{q^m - 1} = 1$ and $(q^t - 1) \mid (q^m - 1)$, which can only happen if $t \mid m$ (**HW**). □

Corollary 43. *In $\mathbb{F}_q[x]$, $x^{q^m} - x = \prod h(x)$ where the product runs over all irreducible polynomials with degree dividing m.*

Define the order $o(f)$ of an irreducible polynomial $f(x) \in \mathbb{F}_q[x]$ as the order of any of its roots in $\mathbb{F}_{q^m} = \mathbb{F}_q[x]/(f(x))$.

Proposition 44. *Let $f(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial with $deg(f(x)) = m$ and $o(f) = e$.*

a) *$o(f) \mid q^m - 1$;*
b) *$f(x) \mid x^{o(f)} - 1$;*
c) *$o(f) \mid n \Leftrightarrow f(x) \mid (x^n - 1)$:*

Proof. **HW**. □

The order of $f(x)$ determines its degree:

Theorem 45. *Let $f(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial with $deg(f(x)) = m$ and $o(f) = e$. Then $m = \text{ord}_e(q)$, ie, m is the least positive integer satisfying $e \mid (q^m - 1)$.*

Proof. **HW**. □

However, $deg(f(x))$ does not determine $o(f)$. Consider for example (**HW**) the polynomials over $\mathbb{F}_2$

$$f(x) = x^4 + x + 1, \qquad g(x) = x^4 + x^3 + x^2 + x + 1.$$

But it is possible to determine $o(f)$ in the following way: $o(f) \mid (q^m - 1)$ so, if $q^m - 1 = \prod_i p_i^{k_i}$ is the prime factor decomposition, we must have $o(f) = \prod_i p_i^{t_i}$ with $t_i \leq k_i$; in fact,

$$t_i = k_i - \max\left\{ s : o(f) \mid \frac{q^m - 1}{p_i^s} \right\}.$$

By Proposition 39,

$$o(f) \mid \frac{q^m - 1}{p_i^s} \Leftrightarrow f(x) \mid \left(x^{\frac{q^m - 1}{p_i^s}} - 1 \right),$$

and we may determine t_i by a sequence of polynomial divisions.

At this point, we may clarify the claim of uniqueness of finite fields:

Theorem 46. *Let q be a prime and $m \geq 1$. There exists a unique, up to isomorphism, field $\mathbb{F}_{q^m}$ with cardinality q^m.*

Proof. The existence of the field follows from the existence of an irreducible polynomial $f(x) \in \mathbb{F}_q[x]$ with degree m.
As to uniqueness, suppose that $f(x)$ and $g(x)$ are two irreducible polynomials of the same degree m. Let α be a primitive element of $\mathbb{F}_q[x]/(f(x))$ and $\mathbb{F}_q[x]/(g(x)) = \mathbb{F}_q[\beta]$. We have the decomposition into irreducible factors $x^{q^m-1} - 1 = \prod_i p_i(x)$, where the $p_i(x)$ are minimal polynomials of its roots. $g(x)$ divides $x^{q^m-1} - 1$, so we must have $g(x) = p_i(x)$ for some i, ie, $g(x)$ is the minimal polynomial of α^i for some i, ie, $\mathbb{F}_q[\beta] \simeq \mathbb{F}_q[\alpha^i] \subset \mathbb{F}_q[\alpha]$. But the two fields have the same cardinality so we have equality. □

We end this section by answering the question of how does an irreducible polynomial over a finite field $\mathbb{F}$ factor in an extension of it. To simplify the notation, we will denote as $\mathbb{F}_m$ a finite field, where of course m is a power of a prime q.

Theorem 47. *Let $\mathbb{F}_m$ be a finite field and $\mathbb{F}_{m^n}$ an extension. Suppose $f(x) \in \mathbb{F}_m[x]$ is an irreducible polynomial with degree t and let $d = \gcd(t, n)$.*
Then $f(x)$ factors in $\mathbb{F}_{m^n}[x]$ as the product of d polynomials, each with degree $\frac{t}{d}$.
In particular, $f(x)$ remains irreducible over $\mathbb{F}_{m^n}$ if and only if $\gcd(t, n) = 1$.

Proof. Suppose that $g(x)$ is an irreducible factor of $f(x)$ in $\mathbb{F}_{m^n}[x]$ with degree s. It suffices to show that $s = \frac{t}{d}$.
First, notice that if $\mathbb{F}_{m^{ns}} = \mathbb{F}_{m^n}[x]/(g(x)) = \mathbb{F}_{m^n}[\alpha]$, ie, α is a root of $g(x)$ in $\mathbb{F}_{m^n}[x]/(g(x))$, then α is also a root of $f(x)$ and so $\mathbb{F}_{m^t} = \mathbb{F}_m[x]/(f(x)) = \mathbb{F}_m[\alpha]$ is a subfield of $\mathbb{F}_{m^{ns}} = \mathbb{F}_{m^n}[\alpha]$. In particular, $t \mid (ns)$ which implies $\frac{t}{d} \mid s$.
Now, let $u = \mathrm{ord}(f)$; this implies, by Theorem 38 above, that $t = \mathrm{ord}_u(m)$. But then α has order u, both as an element of $\mathbb{F}_m[x]/(f(x)) = \mathbb{F}_m[\alpha]$ and of $\mathbb{F}_{m^n}[x]/(g(x)) = \mathbb{F}_{m^n}[\alpha]$, implying that $s = \mathrm{ord}_u(m^n)$. But the properties of multiplicative order imply that

$$\mathrm{ord}_u(m^n) = \frac{\mathrm{ord}_u(m)}{\gcd(\mathrm{ord}_u(m), n)} = \frac{t}{d}.$$

□

1.5.2. *Cyclotomic cosets and Factorizaton.* Given a primitive element α of $\mathbb{F}$, we may compute the minimal polynomial $p_{\alpha^i}(x)$ (which we will denote now simply by $p_i(x)$) of any other nonzero element, using the notion of cyclotomic cosets:

Definition 48. *For any n co-prime to q, the **cyclotomic coset** of i modulo n, with respect to q, is*

$$C_i = \{iq^j \mod n : j \geq 0\};$$

in other words, C_i is the orbit of $i \in \mathbb{Z}_{/n}$ under the mapping

$$\mathbb{Z}_{/n} \to \mathbb{Z}_{/n} \; x \to xq.$$

Obviously, the cyclotomic cosets partition $\mathbb{Z}_{/n}$; $\{i_1, \cdots, i_s\}$ is called a **complete set of representatives** of cyclotomic cosets if $\{C_{i_1}, \cdots, C_{i_s}\}$ are a partition of $\mathbb{Z}_{/n}$.

Example 49. *The cyclotomic cosets modulo* 26 *with respect to* 3*:*

$$\{0\}, \{1,3,9\}, \{2,6,18\}, \{4,12,10\}, \{5,15,19\},$$

$$\{7,21,11\}, \{8,24,20\}, \{13\}, \{14,16,22\}, \{17,25,23\}.$$

The cyclotomic cosets modulo 16 *with respect to* 3*:*

$$\{0\}, \{1,3,9,11\}, \{2,6\}, \{4,12\}, \{5,15,13,7\}, \{8\}, \{10,14\}.$$

Remark 50. *Let m be the order of q in $\mathbb{Z}^{\times}_{/n}$, ie m, the minimal positive integer such that $n \mid (q^m - 1)$. If C_i is the cyclotomic coset of i modulo n, with respect to q, it is clear that $|C_i| = u$ where u is the least positive integer such that*

$$i(q^u - 1) \equiv 0 \mod n;$$

it follows that $|C_i| = m$ if $\gcd(i,n) = 1$; on the other hand, if $\gcd(i,n) = v > 1$ and $n_1 = n/v$, then we get from the same equation that $|C_i| = p$ where p is the order of q in $\mathbb{Z}_{n_1}$ and so, in any case, $p \mid m$.

The next theorem generalizes the factorization of $f(x)$ in $\mathbb{F}_q[x]/(f(x))$ identified before:

Theorem 51. *Let α be a primitive element of $\mathbb{F}_{q^m}$. The minimal polynomial of α^i over $\mathbb{F}_q$ is*

$$p_i(x) = \prod_{j \in C_i} (x - \alpha^j),$$

where C_i is the cyclotomic coset of i modulo $q^m - 1$, with respect to q.

Proof. α^i is obviously a root of the given polynomial. We verify that

$p_i(x) \in \mathbb{F}_q[x]$;
$p_i(x)$ has no multiple roots;
any polynomial $f(x)$ that has α^i as a root is divisible by $p_i(x)$.

□

The details of the proof are left as an exercise (**HW**).

Corollary 52. *Let α be a primitive element of $\mathbb{F}_{q^m}$ and $\{i_1, \cdots, i_r\}$ a complete set of representatives of the cyclotomic cosets modulo $q^m - 1$, with respect to q. Then*

$$x^{q^m-1} - 1 = \prod_{k=1}^{r} p_{i_k}(x).$$

Example 53. *$p(x) = x^3 + 2x + 1$ is irreducible over $\mathbb{F}_3$, so we may take $\mathbb{F}_{27}$ to be $\mathbb{F}_3[\alpha]$ where α is a root of $p(x)$. It turns out that α is also a primitive element. The following table gives the correspondence between powers of α and the expression of the same element on the basis $1, \alpha, \alpha^2$:*

0	1	9	$\alpha + 1$	18	$\alpha^2 + 2\alpha + 1$
1	α	10	$\alpha^2 + \alpha$	19	$2\alpha^2 + 2\alpha + 2$
2	α^2	11	$\alpha^2 + \alpha + 2$	20	$2\alpha^2 + \alpha + 1$
3	$\alpha + 2$	12	$\alpha^2 + 2$	21	$\alpha^2 + 1$
4	$\alpha^2 + 2\alpha$	13	2	22	$2\alpha + 2$
5	$2\alpha^2 + \alpha + 2$	14	2α	23	$2\alpha^2 + 2\alpha$
6	$\alpha^2 + \alpha + 1$	15	$2\alpha^2$	24	$2\alpha^2 + 2\alpha + 1$
7	$\alpha^2 + 2\alpha + 2$	16	$2\alpha + 1$	25	$2\alpha^2 + 1$
8	$2\alpha^2 + 2$	17	$2\alpha^2 + \alpha$		

The cyclotomic cosets found before allow us to factor $x^{26} - 1$ over $\mathbb{F}_3$:

$$\begin{array}{rl} \{0\} & x - 1 \\ \{1, 3, 9\} & (x - \alpha)(x - \alpha^3)(x - \alpha^9) = x^3 + 2x + 1 \\ \{2, 6, 18\} & (x - \alpha^2)(x - \alpha^6)(x - \alpha^{18}) = x^3 + x^2 + x + 2 \\ \{4, 12, 10\} & (x - \alpha^4)(x - \alpha^{12})(x - \alpha^{10}) = x^3 + x^2 + 2 \\ \{5, 15, 19\} & (x - \alpha^5)(x - \alpha^{15})(x - \alpha^{19}) = x^3 + 2x^2 + x + 1 \\ \ldots & \ldots \end{array}$$

1.5.3. *Roots of unity and factorization of $x^n - 1$.* An element $a \in \mathbb{F}^\times$ is a n-root of unity if $a^n = 1$ and a primitive n-root of unity if $ord(a) = n$.
If $\mathbb{F} = \mathbb{F}_{q^m}$ then the multiplicative group $\mathbb{F}^\times$ contains as a subgroup the n-roots of unity if and only if $n \mid (q^m - 1)$. In particular, $\gcd(n, q) = 1$; in fact, if $n = q^t u$ with $\gcd(u, q) = 1$, a n-root of unity in $\mathbb{F}$ is also a u-root of unity.
The smallest extension of $\mathbb{F}_q$ containing the n-roots of unity is $\mathbb{F}_{q^m}$ with $m = \mathrm{ord}_n(q)$. If β is a primitive element (ie a primitive $q^m - 1$ root of unity) the primitive n-roots of unity are (**HW**)

$$\{\beta^k | k = \frac{q^m - 1}{n} t; 1 \leq t < n; \gcd(t, n) = 1\}.$$

We have also the following generalization of Corollary 43:

Theorem 54. *Suppose that $\gcd(q, n) = 1$ and that m is the order of q in $\mathbb{Z}_n^\times$. Let α be a primitive element of $\mathbb{F}_{q^m}$ and $\{i_1, \cdots, i_r\}$ a complete set of representatives of the cyclotomic cosets modulo n, with respect to q. Then the following factorization holds in $\mathbb{F}_q[x]$:*

$$x^n - 1 = \prod_{j=1}^{r} p_{i_j s}(x)$$

where $s = \frac{q^m - 1}{n}$ where $p_l(x)$ is the minimal polynomial of α^l.

Proof. Under the conditions in the statement, α^s is a primitive n-th root of identity in $\mathbb{F}_q[\alpha]$ and so, over this field,

$$x^n - 1 = \prod_{j=0}^{n-1}(x - \alpha^{js});$$

the n exponent values are partitioned as a disjoint union of cyclotomic cosets modulo $q^m - 1$ because if a coset contains a multiple of s then all its elements are also multiples of s; on the other hand, the mapping

$$\mathbb{Z}_{/n} \to \mathbb{Z}_{/(q^m-1)}, \qquad i \to is$$

is well defined, injective, and it preserves cyclotomic cosets with respect to q, ie, i and j are in the same coset modulo n if and only if is and js are in the same coset modulo $q^m - 1$; this implies that a complete system of representatives of cosets modulo n corresponds, by this map, to a complete system of representatives of the cosets modulo $q^m - 1$ that contain the multiples of s.
So, for each $1 \leq v \leq r$, we obtain an irreducible factor

$$p_{i_v s}(x) = \prod_{i \in C_{i_v s}} (x - \alpha^i)$$

where $C_{i_v s}$ denotes the cyclotomic coset modulo $q^m - 1$; if $|C_{i_v s}| = h$,

$$p_{i_v s}(x) = \prod_{j=0}^{h-1}(x - \alpha^{i_v s q^j}).$$

The details of the argument are left as an exercise (**HW**). □

Example 55. *Consider the polynomial $x^{16} - 1 \in \mathbb{F}_3[x]$; a complete system of representatives for the cyclotomic cosets modulo 16, with respect to $q = 3$, was obtained above: $\{0, 1, 2, 4, 5, 8, 10\}$. As $3^4 - 1 = 16 \times 5$, we must use a primitive element α of $\mathbb{F}_{81}$.*
Define $\mathbb{F}_{81} = \mathbb{F}_3[x]/(x^4 + x + 2) = \mathbb{F}_3[\alpha]$. By the previous theorem, we have the factorization

$$x^{16} - 1 = p_0(x)p_5(x)p_{10}(x)p_{20}(x)p_{25}(x)p_{40}(x)p_{50}(x),$$

and, for instance,

$$p_0(x) = (x - \alpha^0) = x - 1$$

while

$$p_{10}(x) = (x - \alpha^{10})(x - \alpha^{30}) = x^2 - (\alpha^{10} + \alpha^{30})x + \alpha^{40} = x^2 + x + 2$$

*The computation of the other factors is left as an exercise (**HW**).*

The method of cyclotomic cosets to factor polynomials $x^n - 1$, with $n \mid (q^m - 1)$ into irreducible factors (which are minimal polynomials of their roots) has the disadvantage of depending on computations envolving a primitive element of the extension field. This disadvantage is stressed by the fact that there is no general method to find primitive elements, even for prime fields.
The next two subsections are devoted to the application of other mathematical concepts and theories to the problem of determining irreducible polynomials.

1.5.4. *Cyclotomic Polynomials.* It is possible to obtain partial factorizations of $x^n - 1$ working only in $\mathbb{F}_q[x]$ using the theory of cyclotomic polynomials.
Let $\mathbb{F}$ be any field containing the group of n-th roots of unity, or more precisely an isomorphic copy of it. This may be $\mathbb{C}$ but it may also be $\mathbb{F}_{q^m}$ for m such that $n \mid q^m - 1$.

Definition 56. *Let $n \mid (q^m - 1)$. The n-th cyclotomic polynomial over $\mathbb{F}_{q^m}$ is defined as $\Phi_n(x) = \prod_{a:\mathrm{ord}(a)=n}(x - a)$.*

Although our definition depends on the extension field containing the n-roots of unity, we'll see that the cyclotomic polynomials do not depend on that choice. We start with the following result:

Theorem 57. *$\Phi_n(x) \in \mathbb{F}_q[x]$ and its degree is $\phi(n)$. Moreover $x^n - 1 = \prod_{d|n} \Phi_d(x)$.*

Proof. **HW**. □

The same argument used in the proof of the second version of Möbius Inversion Formula gives us an explicit formula for the cyclotomic polynomials:

Proposition 58. *For $n \in \mathbb{Z}^+$,*

$$\Phi_n(x) = \prod_{d|n}(x^{n/d} - 1)^{\mu(d)}.$$

Proof. **HW**. □

As a consequence, we have

Lemma 59. *Let p be prime and $n, k \in \mathbb{Z}+$. Then*

1. $\Phi_{pn}(x) = \begin{cases} \Phi_n(x^p) \text{ if } p \mid n \\ \frac{\Phi_n(x^p)}{\Phi_n(x)} \text{ if } p \nmid n \end{cases}$
2. $\Phi_{p^k n}(x) = \begin{cases} \Phi_n(x^{p^k}) \text{ if } p \mid n \\ \frac{\Phi_n(x^{p^k})}{\Phi_n(x^{p^{k-1}})} \text{ if } p \nmid n \end{cases}$

Proof. **HW**. **Hint:** In 1. apply the Inversion Formula for cyclotomic polynomials. In the case $p \mid n$, notice that if $d \mid pn$ then either $d \mid n$ or $d \nmid n$ and $p^2 \mid d$; in the case $p \nmid n$, notice that the divisors of pn are either divisors of n or of the for pd with $d \mid n$.
2. is a easy consequence of 1. □

We have the following theorem, which we state without proof:

Theorem 60. *For $n \in \mathbb{Z}^+$, $\Phi_n(x)$ is irreducible over $\mathbb{Z}$.*

However, the cyclotomic polynomials $\Phi_n(x)$ are not, in general, irreducible over $\mathbb{F}_q$: consider, for example, the case $n = q^m - 1$; then, assuming that α is a primitive element in $\mathbb{F} = \mathbb{F}_{q^m}$, we have the factorization

$$\Phi_n(x) = \prod_{0<i<q^m-1;\gcd(i,q^m-1)=1} (x - \alpha^i);$$

but the minimal polynomial of each of these α^i over $\mathbb{F}_q$ has degree m. We conclude that, over this field, $\Phi_{q^m-1}(x)$ factors as a product of degree m irreducible polynomials.
But the fact that a degree m irreducible polynomial $f(x) \in \mathbb{F}_q[x]$ totally splits in $\mathbb{F}_{q^m}$ (or in any extension field containing it) and that all its roots have the same order, implies that if $f(x)$ is a factor of some $x^n - 1$ then it must be a factor of one of the cyclotomic polynomials $\Phi_d(x)$ with $d \mid n$.

1.5.5. *Minimal polynomials by Linear Algebra.* A Linear Algebra approach to the computation of irreducible polynomials over finite fields is as follows: let $\alpha \in \mathbb{F}_q[\beta] = \mathbb{F}_q[x]/(f(x))$, where $f(x)$ is an irreducible polynomial of degree m. As it was seen above, $1, \beta, \cdots, \beta^{m-1}$ is a basis of the $\mathbb{F}_q$ vector space $\mathbb{F}_q[\beta]$. In particular, we have a matrix M such that

$$(1, \alpha, \alpha^2, \cdots, \alpha^m) = (1, \beta, \cdots, \beta^{m-1})M.$$

It is then clear (**HW**) that a polynomial $p(x) = \sum_{i=0}^{m} a_i x^i \in \mathbb{F}_q[x]$ satisfies $p(\alpha) = 0$ if and only if

$$M \begin{pmatrix} a_0 \\ \vdots \\ a_m \end{pmatrix} = 0.$$

So to find the minimal polynomial of α corresponds to determine the solution $(a_0, \cdots, a_m)^t$ of this last equation such that there exists k for which $a_k = 1$, $a_i = 0$ for $i > k$, with k minimal. This can be done applying row-reduction to M, obtaining a matrix of the form

$$\begin{bmatrix} I & U \\ 0 & V \end{bmatrix}$$

where I is the k-dimensional identity matrix, and the first column of U is nonzero. The solution wanted is then easily obtained (**HW**).

Exercise 61. *Let $\mathbb{F}_3[\beta]$ be defined by $\beta^3 = \beta + 2$, and $\alpha = \beta^2 + \beta + 2$. Compute the minimal polynomial of α by the method described in this subsection.*
In an example above, it was seen, by a direct computation, that β (denoted as α in that example) is in fact a primitive element of the field. Use the table given there and the rsults about cyclotomic cosets to confirm the result.

1.5.6. *Rabin's Criterion for Irreducibility.* Although the results in previous sections may help in identifying irreducibility, they do not provide a general criterion and/or method. One such criterion was proposed by Rabin:

Proposition 62. *Let $f(x) \in \mathbb{F}_q[x]$ be a degree m polynomial, $\{p_1, \cdots, p_t\}$ the primes dividing m, and $m_i = \frac{m}{p_i}$. Then $f(x)$ is irreducible if and only if*

i) $f(x) \mid (x^{q^m} - x)$;
ii) *For all* $1 \leq i \leq t$, $\gcd(f(x), x^{q^{m_i}} - x) = 1$.

Proof. Suppose $f(x)$ is irreducible; then it obviously satisfies i) and ii) (**HW**). Suppose, on the other hand that $f(x)$ satisfies i) and ii). Then, by Fermat-Euler Theorem, $f(x)$ totally splits in $\mathbb{F}_{q^m}$; if $f(x)$ has an irreducible factor $g(x)$ with degree $n < m$ then $\mathbb{F}_{q^n} = \mathbb{F}_q[x]/(g(x))$ is a subfield of $\mathbb{F}_{q^m}$ and so $n \mid m$. But then $n \mid m_i$ for some $1 \leq i \leq t$; this would imply $\mathbb{F}_{q^n} \subset \mathbb{F}_{q^{m_i}}$ and in particular $g(x) \mid \gcd(f(x), x^{q^{m_i}} - x)$, contradicting ii).
The details of the argument are left as an exercise (**HW**). □

1.6. **Automorphisms, Norm and Trace.** This subsection collects some basic results on the group of automorphisms of an extension F_{q^m} of a prime field $\mathbb{F}_q$ and on the Norm and Trace maps associated to it. Many details are left as an exercise.

Recall that a map $\tau : F_{q^m} \to F_{q^m}$ is an automorphism if it is a bijection satisfying

$$\tau(x+y) = \tau(x) + \tau(y), \qquad \tau(xy) = \tau(x)\tau(y), \qquad \forall x, y \in \mathbb{F}_{q^m}.$$

Definition 63. *$Gal(F_{q^m}/\mathbb{F}_q)$ denotes the group of automorphisms of F_{q^m} that leave the points of $\mathbb{F}_q$ fixed.*

As we saw above, an example of such an automorphism is the Frobenius automorphism σ. We will see that in fact $Gal(F_{q^m}/\mathbb{F}_q) = \{\sigma^k : 0 \leq k < m\}$, where, of course, σ^k denotes de k-fold composition of σ.

By definition, each $\varphi \in Gal(F_{q^m}/\mathbb{F}_q)$ is a linear invertible transformation of F_{q^m}, as a vector space over $\mathbb{F}_q$ (**HW**). The set $L(F_{q^m})$ of all $\mathbb{F}_q$-linear transformations of F_{q^m} is also a vector space over F_{q^m}, and we have

Lemma 64. *The automorphisms in $Gal(F_{q^m}/\mathbb{F}_q)$ are linearly independent over $\mathbb{F}_{q^m}$ (as elements of $L(F_{q^m})$).*

Proof. Assume $\varphi_1, \cdots, \varphi_r \in Gal(F_{q^m}/\mathbb{F}_q)$ and $a_1, \cdots, a_r \in \mathbb{F}_{q^m}^{\times}$. are such that

$$a_1\varphi_1 + \cdots + a_r\varphi_r = 0$$

is a shortest nontrivial linear relation. Obviously $r > 1$ and the φ_i are all distinct. Let $x \in \mathbb{F}_{q^m}$ be some element such that $\varphi_1(x) \neq \varphi_2(x)$. Then, for any $y \in \mathbb{F}_{q^m}$,

$$\sum_{i=1}^{r} a_i\varphi_i(xy) = \sum_{i=1}^{r} a_i\varphi_i(x)\varphi_i(y) = 0$$

which implies that $\sum_{i=1}^{r} a_i\varphi_i(x)\varphi_i = 0$ is also a linear relation. But then

$$\sum_{i=2}^{r} a_i(\varphi_i(x) - \varphi_1(x))\varphi_i = 0$$

is a shorter linear relation, a contradiction. □

As a consequence,

Lemma 65. *$Gal(F_{q^m}/\mathbb{F}_q)$ contains at most m elements.*

Proof. Suppose that this is not the case and let $\varphi_1, \cdots, \varphi_n$ be distinct elements of $Gal(F_{q^m}/\mathbb{F}_q)$, with $n > m$. If $v_1, \cdots, v_m$ is a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, then the system of m linear equations (over $\mathbb{F}_{q^m}$) in n variables

$$\begin{pmatrix} \varphi_1(v_1) & \varphi_2(v_1) & \cdots & \varphi_n(v_1) \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_1(v_m) & \varphi_2(v_m) & \cdots & \varphi_n(v_m) \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

must have a nontrivial solution $(a_1, \cdots, a_n)$. This implies that $\sum_{i=1}^{n} a_i \varphi_i(y) = 0$, for any $y \in \mathbb{F}_{q^m}$, ie, the automorphisms φ_i are linearly dependent, contradicting the result in the previous lemma. □

Corollary 66. *$Gal(F_{q^m}/\mathbb{F}_q) = \{\sigma^k : 0 \leq k < m\}$, where σ is the Frobenius automorphism*

$$\sigma : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}, \qquad \sigma(x) = x^q.$$

The norm and trace maps associated to the extension are fundamental in the theory of finite fields and will play also a role in the applications to coding.
Their definition and main properties arelisted in the propositions below.

Proposition 67. *The **Trace** map, defined by*

$$Tr(a) = \sum_{j=0}^{m-1} a^{q^j} = \sum_{j=0}^{m-1} \sigma^j(a),$$

satisfies

i) $Tr(a) \in \mathbb{F}_q \ \forall a \in \mathbb{F}_{q^m}$;
ii) $Tr(a+b) = Tr(a) + Tr(b) \ \forall a, b \in \mathbb{F}_{q^m}$;
iii) $Tr(ta) = tTr(a) \ \forall t \in \mathbb{F}_q, \ \forall a \in \mathbb{F}_{q^m}$;
iv) *For each $t \in \mathbb{F}_q$, $Tr(x) = t$ has q^{m-1} distinct solutions.*
v) $Tr(x) = 0 \Leftrightarrow x = y - y^q$, *for some $y \in \mathbb{F}_{q^m}$.*

Proof. (**HW**). □

In other words, Tr is a surjective linear mapping from the $\mathbb{F}_q$-vector space $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$, with kernel

$$y - y^q : y \in \mathbb{F}_{q^m}.$$

Proposition 68. *The **Norm** map, defined by*

$$N(a) = \prod_{j=0}^{m-1} \sigma^j(a), \qquad \forall$$

is a surjective homomorphism from $\mathbb{F}_{q^m}^{\times}$ to $\mathbb{F}_q^{\times}$ (both multiplicative groups) with kernel

$$\{\frac{x}{\sigma(x)} : x \in \mathbb{F}_{q^m}^{\times}\}.$$

Proof. (**HW**). □

1.7. **Supplementary Results and Problems.**

Lemma 69. *For any $q, u, v > 1$, $\gcd(q^u - 1, q^v - 1) = q^{\gcd(u,v)} - 1$.*

Proof. **HW**. **Hint:** Analise the application of Euclides's algorithm to the two pairs of integers □

Problem 70. *Find a primitive element and construct a logarithmic table for (some isomorphic copy of) $\mathbb{F}_{25}$.*

Problem 71. *Find the irreducible factors of $x^{24} - 1$ over $\mathbb{Z}$ and over $\mathbb{F}_7$.*

Problem 72. *Verify if each one of the following polynomials is irreducible over $\mathbb{F}_2$:*

a) $x^4 + x^3 + 1$;
b) $x^8 + x^7 + x^6 + x^5 + x^4 + x + 1$.

Problem 73. *Compute the decomposition $x^9 - 1 = \prod_{d|9} \Phi_d(x)$.*
Compute the cyclotomic cosets modulo $n = 9$ with respect to $q = 2$ and use them to justify that the factors in the previous decomposition are irreducible in $\mathbb{F}_2[x]$.

Problem 74. *The application of Rabin's result to determine if a given polynomial is irreducible may involve computations with polynomials of reasonably large degree, requiring a computer.Sometimes a more elementary approach solves the problem. Verify that the polynomial $p(x) = x^4 + x^2 + 2$ is irreducible over $\mathbb{F}_5$:*

i) *Verify that $p(x)$ has no factors of degree 1;*
ii) *Write $p(x)$ as a product of two degree 2 polynomials and derive a contradiction.*

Repeat the exercise for $p(x) = x^4 + x^3 + 1$.

Problem 75. *Determine the order of each one of following polynomials*

a) $x^6 + x + 1 \in \mathbb{F}_2[x]$;
b) $x^6 + x^4 + x^2 + x + 1 \in \mathbb{F}_2[x]$;
c) $x^4 + x + 2 \in F_3[x]$;
d) $x^5 + 2x + 1 \in F_3[x]$:

Problem 76. *Let $\mathbb{F}_2[\alpha]$ be defined as $\mathbb{F}_2[x]/(x^5 + x^2 + 1)$ (ie, $\alpha^5 + \alpha^2 + 1 = 0$). Is this a field? Is it a direct sum of fields?*
Rewrite as a sum of monomials with coefficients in $\mathbb{F}_2$ the polynomial

$$(x - \alpha)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8)(x - \alpha^{16}).$$

1.7.1. *Hermitian Inner product.* It is possible to define other inner products other than the canonical one. An example is the following

Definition 77. *Let* $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ *where* $\alpha^2 = \alpha + 1$. *Define the conjugate map* $a \to \bar{a}$ *by*

$$\bar{0} = 0, \qquad \bar{1} = 1, \qquad \bar{\alpha} = \alpha^2, \qquad \bar{\alpha^2} = \alpha.$$

Given $x, y \in \mathbb{F}_4^n$, *their Hermitian inner product is*

$$< x, y >_H = \sum_i x_i \bar{y_i}.$$

Exercise 78. *Prove that* $< , >_H$ *has the properties of an inner product.*

The **hexacode** is the $[6, 3, 4]$ code over $\mathbb{F}_4$ with generator

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & \alpha & \alpha \\ 0 & 1 & 0 & \alpha & 1 & \alpha \\ 0 & 0 & 1 & \alpha & \alpha & 1 \end{bmatrix}$$

Exercise 79. *Prove that the hexacode is not self-dal with respect to the usual inner product but is self-dual with respect to the Hermitian inner product.*